

UNITED STATES PATENT APPLICATION

**SERVICE SELECTION IN A SHARED ACCESS NETWORK
USING TUNNELING**

INVENTORS:

John W. Garrett

Charles Robert Kalmanek Jr.

Han Q. Nguyen

Kadangode K. Ramakrishnan

Cross Reference to Related Applications

This application claims priority to United States Provisional Application Serial No. 60/190,633, entitled "INTERNET SERVICE SELECTION OVER CABLE," filed on March 20, 2000, and to United States Provisional Application Serial No. 60/190,636, entitled "QUALITY OF SERVICE OVER THE HFC CABLE PLANT," filed on March 20, 2000, the contents of which are incorporated by reference herein.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
22

SERVICE SELECTION IN A SHARED ACCESS NETWORK USING TUNNELING

Field of the Invention

5 The present invention relates generally to communication network services, and, more particularly, to providing multiple services in a communication network.

Background of the Invention

10 Customers of communication network services often desire access to a plurality of different services and different service providers. For example, when using a dial-up connection to a packet-switched data network such as the Internet, a customer can choose from multiple service providers by dialing different telephone numbers in the PSTN. The physical path from the customer to
15 the customer's Internet Service Provider (ISP) is dedicated to the connection for the duration of the telephone call. The ISP assigns an IP address to the customer and can link the authenticated customer and the assigned IP address to the physical address (e.g. dial-up modem) used by the customer. With this linkage, the ISP can ensure the customer only uses the address authorized by the ISP and
20 can use the customer's IP address to manage access to the ISP's services. The physical connection between a customer and the ISP, as well as the linkage to IP address assignment and customer authentication is terminated when the dial-up connection is terminated.

 Constrained by the physical capacity of these temporary
25 connections across the PSTN, many service providers are moving to high-speed access architectures (e.g., digital subscriber line (DSL), wireless, satellite, or cable) that provide dedicated physical connectivity directly to the subscriber and under the control of the ISP. These alternatives to shared access through the switched telephone network, however, do not lend themselves to shared access by
30 multiple services and/or service providers.

Summary of the Invention

It is an object of the invention to enable multiple services or service providers to share the facilities of an access network infrastructure providing physical connectivity to subscribers. In accordance with an embodiment of the invention, each network access device is assigned two network addresses: a first network address associated with a particular service or service provider to which the user of the device is subscribed and a second network address utilized in the access network infrastructure to tunnel to the relevant service network. Packets from the network access device are encapsulated and routed through the access network infrastructure to arrive at a network node within the associated service network where it is de-encapsulated and routed to its destination. The network access device advantageously may be used in communication network services with a service or service provider that is separate from the operator of the access network infrastructure.

These and other advantages of the invention will be apparent to those of ordinary skill in the art by reference to the following detailed description and the accompanying drawings.

Brief Description of the Drawings

FIG. 1 illustrates an interconnection of packet-switched service networks and an access network embodying principles of the invention.

FIG. 2A and FIG. 2B is conceptual representation of an example embodiment using layer three tunneling illustrating principles of the invention based on an HFC access architecture with corresponding end-to-end protocol layers.

FIG. 3A and FIG. 3B is conceptual representation of another example embodiment using layer two tunneling illustrating principles of the invention based on an HFC access architecture with corresponding end-to-end protocol layers.

FIG. 4 is a conceptual representation of IP encapsulation within IP.

FIG. 5 is a conceptual representation of minimal encapsulation within IP.

FIG. 4 is a flowchart of processing performed at a network access device, in accordance with an embodiment of the invention.

FIG. 5 is a flowchart of processing performed at a tunneling router in the service network, in accordance with an embodiment of the invention.

Detailed Description

In FIG. 1, a plurality of subscribers operating network access devices 101, 102, 103, ... 104 are provided access to communication network services, which are facilitated by a plurality of packet-switched data networks, shown in FIG. 1 as 151 and 152. Packet-switched data networks 151 and 152, referred to herein as "service networks," offer access to different services and/or are operated by different service providers. For example, service network 151 could provide packet-switched connectivity to public data networks while service network 152 could offer packet-switched telephony service (or the same public data network connectivity, but from a different service provider). The service networks, as is well known in the art, utilize a network addressing scheme to route datagrams to and from hosts: for example, where the service networks utilize the TCP/IP protocol suite, Internet Protocol (IP) addresses are assigned to each host and utilized in the process of routing packets from a source to a destination in the networks. See, e.g., "INTERNET PROTOCOL," IETF Network Working Group, RFC 791 (September 1981); S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," IETF Network Working Group, RFC 1883 (December 1995), which are incorporated by reference herein. The invention shall be described herein with particular reference to the TCP/IP protocol suite and IP addresses, although those skilled in the art would readily be able to implement the invention using any of a number of different communication protocols.

The network access devices 101 ... 104 are typically customer premises equipment (CPE) such as a personal computer, information appliance, personal data assistant, data-enabled wireless handset, or any other type of device

capable of accessing information through a packet-switched data network. Each network access device 101 ... 104 is either connected to or integrated with a network interface unit 111 ... 114, e.g. a modem, which enables communication through an access network infrastructure, shown as 120 in FIG. 1. The access network infrastructure 120 advantageously can be operated and maintained by an entity that is the same as or different from the entities operating and maintaining the service networks 151 and 152. The network access devices 101 ... 104, in accordance with an aspect of the invention, communicate with the packet-switched service networks 151 and/or 152 by what is known in the art as "tunneling." Tunneling is the process by which a packet is encapsulated within another packet, which is delivered between two endpoints of the "tunnel" as a means to alter the conventional routing of the packet. The encapsulated packet travels to an intermediate destination that otherwise would not have been selected based on the destination address indicated in the encapsulated packet. Thus, service-related network traffic is tunneled between the network access devices 101 ... 104 used by the service subscribers and the service networks 151, 152 providing the relevant services. Each network access device in FIG. 1 is assigned at least two IP addresses: (1) an IP address allocated from the address space of the access network infrastructure (this address is used when tunneling to the relevant service network) and (2) an IP address allocated from an address space associated with the particular service or service provider to which the user of the device is subscribed. For example, and for purposes of the description herein, network access device 101 is assumed to have been assigned an IP address associated with the service provider operating service network 151 and an IP address for tunneling to service network 151.

As described in further detail herein, tunneling can be accomplished in different layers of the protocol stack. In one embodiment of the present invention, the technique of IP encapsulation can be utilized—so that the different IP-based services offered by the different service networks 151 and 152 utilize shared layer one and layer two resources in the access network infrastructure 120. FIG. 2A shows an exemplary access architecture for practicing

this embodiment based on a hybrid fiber coaxial (HFC) access network. As is
125 known in the art, each network interface device 201 ... 202 is either connected to
or integrated with a cable modem 211 which enables communication through the
HFC network 221. In accordance with the Data Over Cable Service Interface
Specification (DOCSIS), a Cable Modem Termination System (CMTS), shown as
225 in FIG. 2A, communicates with the cable modems 211 and manages access to
130 both upstream and downstream cable capacity on the HFC networks 221. See,
e.g., "Data-Over-Cable Service Interface Specifications: Cable Modem
Termination System – Network Side Interface Specification," Cable Television
Laboratories, Inc., SP-CMTS-NSI-I01-960702; "Data-Over-Cable Service
Interface Specifications: Cable Modem to Customer Premise Equipment Interface
135 Specification," Cable Television Laboratories, Inc., SP-CMCI-C02C-991015;
"Data-Over-Cable Service Interface Specifications: Baseline Privacy Plus
Interface Specifications," Cable Television Laboratories, Inc., SP-BPI+-I06-
001215, which are incorporated by reference herein. The CMTS 225 manages
the scheduling of both upstream and downstream transmission and allocates cable
140 capacity to individual customers identified by a Service ID (SID). The CMTS
225 can have an integrated router 228 or can be a separate device 226 that bridges
to a fast Ethernet switch 227 which connects to the router 228. The IP router 228
provides connectivity to an IP network 222 which interfaces to IP routers 241 and
242 in service networks 251 and 252, respectively. Accordingly, the HFC
145 network 221, the CMTS 225, and the IP network 222 correspond to the access
network infrastructure 120 shown in FIG. 1. FIG. 2B shows a conceptual diagram
of the end-to-end communication protocol stack from a network access device 201
(101) to a router 241 (141) in service provider's network 251 (151) where IP
encapsulation is being utilized. As is known in the art, the lowest layer deals with
150 the physical layer (PL) of the protocol stack, e.g. the Ethernet physical media
device (PMD) layer; the second layer deals with the data link layer, e.g. the
Ethernet Media Access Control (MAC) layer; while the third layer in the protocol
stack deals with the network layer, e.g. the IP layer. As shown in the network
layer of the protocol stack in FIG. 2B, IP traffic between the network access

155 device 201 and the router 241 in the service network 251 is encapsulated within another IP layer.

IP encapsulation may be accomplished using a variety of known techniques. FIG. 4 is a conceptual representation of the process of encapsulating a standard IPv4 packet, in accordance with the technique of “IP Encapsulation Within IP.” See C. Perkins, “IP Encapsulation Within IP,” IETF Network Working Group, RFC 2003 (October 1996), which is incorporated by reference herein. The original IP packet includes a header and a data region which constitutes the payload of the IP packet. To encapsulate an IP packet using IP in IP encapsulation, an outer IP header 410 is inserted before the packet’s existing header 420 and data region 405. The outer IP header Source IP Address 403 and Destination IP Address 404 identify the endpoints of the tunnel. The original IP packet remains basically unchanged and can be readily de-capsulated by stripping off the outer IP header 410. FIG. 5 is a conceptual representation of another process of encapsulating a standard IPv4 packet, in accordance with the technique known in the art as “Minimal Encapsulation Within IP.” See C. Perkins, “Minimal Encapsulation Within IP,” IETF Network Working Group, RFC 2004 (October 1996), which is incorporated by reference herein. Minimal encapsulation achieves the same objective as above without actually including the full IP header of the original packet. Instead, the Destination IP Address field 502 of the original packet (and optionally the Source IP Address field 501) is modified to force routing to the intermediate destination—Destination IP Address 504—and the protocol field is modified to indicate that minimal encapsulation is being utilized. The original values of the Destination IP Address field (and the Source IP Address field if needed) and protocol field are saved in an eight or twelve octet extension to the original IP header. The extension and the header are depicted as 520 and 510, respectively, in FIG. 5. The Total Length field of the original packet is also changed to reflect the expanded length, and the Header Checksum recalculated. When the intermediate destination receives the packet, it observes the “minimal encapsulation” protocol field, restores the original packet based on the values carried in the extension 520 to the IP header 510, and forwards the

original packet. Where minimal encapsulation is initiated by an intermediate router, perhaps based on a packet filter, both Source and Destination IP Address fields are modified in the original packet and carried in a twelve octet header extension. If minimal encapsulation is initiated by the source of the packet, there is no need to modify the Source IP Address field in the IP header, and an eight octet minimal encapsulation extension can be added to the IP header. The format of the minimal encapsulation extension 520 to the IP header 510 is shown in FIG. 5. The fields in the extension are defined in RFC 2004 as follows:

PROTOCOL	Copied from the Protocol field in the original IP header.
ORIGINAL SOURCE ADDRESS PRESENT (S) (508 in FIG. 5)	<p>0 The Original Source Address field is not present. The length of the minimal tunneling header in this case is 8 octets.</p> <p>1 The Original Source Address field is present. The length of the minimal tunneling header in this case is 12 octets.</p>
RESERVED	Sent as zero; ignored on reception.
HEADER CHECKSUM	The 16-bit one's complement of the one's complement sum of all 16-bit words in the minimal forwarding header. For purposes of computing the checksum, the value of the checksum field is 0. The IP header and IP payload (after the minimal forwarding header) are not included in this checksum computation.
ORIGINAL DESTINATION ADDRESS (502 in FIG. 5)	Copied from the Destination Address field in the original IP header.
ORIGINAL SOURCE ADDRESS (501 in FIG. 5)	Copied from the Source Address field in the original IP header. This field is present only if the Original Source Address Present (S) bit is set.

195 FIG. 6 and FIG. 7 set forth the processing performed at a network
access device and a service network router, respectively, to force service-related
packets to route through the service network. The network access device has been
pre-configured with its IP address, with its service-related IP address, and with the
IP address of the service network router at the other end of the tunnel. It is
200 advantageous to provide a service activation system which permits the dynamic
allocation, assignment, and reassignment of the IP addresses to the plurality of
network access devices based on customer subscriptions to particular services, as
further described in copending utility patent application, "SERVICE SELECTION
IN A SHARED ACCESS NETWORK USING DYNAMIC HOST
205 CONFIGURATION PROTOCOL," filed contemporaneously with the present
application, and incorporated by reference herein. At step 601, the process
running on the network access device (or alternatively on another device on behalf
of the network access device) receives a packet that has been constructed by
another process or another part of the same process. At step 602, the packet is
210 determined to be service-related and, thus, outbound to the relevant service
network. The packet has the service-related IP address in the source address field
and a destination address. At step 603, the packet is encapsulated using, for
example, the encapsulation techniques described above. The destination address
field of the new packet is the IP address of the service network router. At step
215 604, the encapsulated packet is tunneled to the service network router in the
service network. FIG. 7 sets forth the processing performed at the router in the
service network. At step 701, the router receives an incoming packet. At step
702, the router reads the packet header and retrieves any packet filtering rules
reflected in access lists and the rules provided for encapsulation and de-
220 encapsulation of packets. At step 703, the router compares the destination address
to its own address (or the address of a virtual interface, as further described
herein) and determines whether the packet has been encapsulated. At step 704,
the router decapsulates the packet and routes the packet to the original destination
address field in the packet. Before decapsulating the packet, the router may check

225 through a list of authorized service-related IP addresses to ensure that the packet comes from a properly authenticated subscriber's network access device. The use of encapsulation by the network access device and the service network router is transparent to the access network infrastructure.

Packets directed to the subscriber from the rest of the Internet can
 230 be addressed to the tunneling IP address of the network access device and forwarded using normal routing procedures without tunneling. Where for some reason the service provider wishes to route service-related traffic back through the service network, such packets can be addressed to the service-related IP address and routed back to the service network router. With reference to FIG. 7 again, the
 235 service network router receives the incoming packet at step 701 and determines at step 705 that the destination address of the packet matches a service-related IP address associated with a particular subscriber. At step 706, the router encapsulates the packet using, for example, an encapsulation technique describe above. The router accesses a database of service subscribers and determines the
 240 tunneling IP address associated with the service-related IP address used by the particular subscriber. The router then uses this IP address in the destination field when encapsulating the packet. At step 707, the packet is tunneled to the network access device associated with the subscriber. With reference to FIG. 6 again, the network access device process receives the packet at step 601 and determines at
 245 step 605 that the packet is encapsulated and from the encapsulating router in the service network. At step 606, the packet is decapsulated and processed accordingly by the relevant application.

Any communication between the network access device and devices attached to the access network infrastructure need not use encapsulation.
 250 Such packets can be processed normally by the network access device at step 607 using the non-service-related IP address and routed by the access network infrastructure using normal routing procedures. Note that communications between the network access device and the service network provider itself, e.g. a DNS query, do not need to use tunneling – but could use tunneling depending on
 255 the needs of the different entities.

The service provider router that de-encapsulates packets may be a single point of failure that may block customer access to service provider services. It is advantageous to provide procedures to eliminate this single point of failure. The address used by subscribers to forward packets should be routed to an

260 available router in the service network. One method of accomplishing this is to have the operator of the service network choose a subnet to provide the address of the de-encapsulation router(s). Each de-encapsulation router is configured with a virtual interface with an address on the specified subnet. See, e.g., C. Perkins, "IP Mobility Support," IETF Network Working Group, RFC 2002 (October 1996),

265 which is incorporated by reference herein. No "real" interfaces are allowed on this subnet. Note that a "virtual interface" exists at an IP level for routing purposes, but is not associated with any physical port. Each router advertises connectivity to the specified subnet, but since all interfaces on the subnet are virtual interfaces, there is no local connectivity (via the specified subnet). Routers

270 on this "virtual subnet" need not be "close" to each other in a routing sense. The directed subnet broadcast address (the host part of the address can be all ones) looks like a normal host address to every router that does not know the subnet mask. Therefore a packet addressed to a directed subnet broadcast address will be forwarded to the "closest" router advertising connectivity to the subnet. If a

275 subscriber's network access device uses the directed subnet broadcast address of the subnet shared by de-encapsulation routers as the destination of encapsulated packets, normal routing procedures will forward the packet to the "closest" router advertising connectivity to the subnet. The de-encapsulation router that receives the packet will recognize that the packet is a broadcast, and process the packet

280 (since it has an address on the subnet). Since the interface associated with the subnet is a virtual interface, the router cannot forward the packet to other members of the subnet. Normal routing procedures will ensure that packets are forwarded to the "closest" available de-encapsulation router, advantageously making appropriate adjustments as routers fail and/or recover from failure.

285 The above embodiments have been described from the perspective of layer three tunneling. Another embodiment of this aspect of the invention is to

use a layer two tunneling technique between the network access device and a service network node acting as a layer two tunnel termination device. For example, FIG. 3A sets forth another exemplary access architecture based on an HFC network, roughly corresponding to FIG. 2, using the Layer Two Tunneling Protocol (L2TP). See, e.g., W. Townsley, A. Valencia, G. Zorn, A. Rubens, G. Pall, B. Palter, "Layer Two Tunneling Protocol (L2TP)," IETF Network Working Group, IETF draft, draft-ietf-l2tp-l2tpbis-01.txt (November 2000). Rather than using layer three routers in FIG. 2, the service networks 351 and 352 in FIG. 3 have L2TP Network Servers ("LNS") 341 and 342. An LNS can be a router or other network node configured to act as a layer two tunnel terminating device. FIG. 3B is a conceptual diagram of the end-to-end communication protocol stack from a network access device 301 to an LNS 341 in the service provider's network 351 where L2TP is utilized. The network access device encapsulates PPP packets in L2TP for transport across the access network infrastructure to the relevant service network. The PPP packets are tunneled across the access network infrastructure to an LNS in the service network which strips the L2TP and terminates PPP.

The foregoing Detailed Description is to be understood as being in every respect illustrative and exemplary, but not restrictive, and the scope of the invention disclosed herein is not to be determined from the Detailed Description, but rather from the claims as interpreted according to the full breadth permitted by the patent laws. It is to be understood that the embodiments shown and described herein are only illustrative of the principles of the present invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention. For example, the detailed description describes an embodiment of the invention with particular reference to an HFC access network architecture. However, the principles of the present invention could be readily extended to other access network architectures, such as DSL, wireless, satellite, etc. Such an extension could be readily implemented by one of ordinary skill in the art given the above disclosure.